A novel solution-technique applied to a novel WAAS architecture

Salvatore J. Bavuso NASA Hampton

Key Words: Weibull, Reliability, Monte Carlo, simulation, importance sampling, HARP (Hybrid Automated Reliability Prediction), Fault tree, HIRel (HARP integrated Reliability tool system), WAAS, GPS

ABSTRACT

The Federal Aviation Administration has embarked on an historic task of modernizing and significantly improving the national air transportation system. One system that uses the Global Positioning System (GPS) to determine aircraft navigational information is called the Wide Area Augmentation System (WAAS). This paper describes a reliability assessment of one candidate system architecture for the WAAS. A unique aspect of this study regards the modeling and solution of a candidate system that allows a novel cold sparing scheme. The cold spare is a WAAS communications satellite that is fabricated and launched after a predetermined number of orbiting satellite failures have occurred and after some stochastic fabrication time transpires. Because these satellites are complex systems with redundant components, they exhibit an increasing failure rate with a Weibull time to failure distribution. Moreover, the cold spare satellite build-time is Weibull and upon launch is considered to be a good-as-new system with an increasing failure rate and a Weibull time to failure distribution as well. The reliability model for this system is non-Markovian because three distinct system clocks are required: the time to failure of the orbiting satellites, the build time for the cold spare, and the time to failure for the launched spare satellite. A powerful dynamic fault tree modeling notation and Monte Carlo simulation technique with importance sampling are shown to arrive at a reliability prediction for a 10 year mission.

BACKGROUND

A revolution in terrestrial navigation that promises to significantly change our way of life is occurring and is being made possible by the Global Positioning System (GPS). Twenty four satellites orbit the earth at more than 10,000 miles constantly broadcast radio-navigation signals that shower the entire planet. Sophisticated GPS receivers that can be used to establish latitude and longitude anywhere on the earth are being purchased for under $200 and have become popular with hikers, fisherman, recreational boaters, and general aviation pilots. Even greater impacts are looming in the near future. One of these is the national air traffic control system. The Federal Aviation Administration has embarked on an historic task of modernizing and significantly improving the national air transportation system (Ref. 1). The envisioned improvements are designed to enable the FAA to better manage the ever increasing growth in air traffic and thereby increase air traffic safety and reduce operational costs. The key element in the FAA's plan is GPS which interacts with two revolutionary systems and an operational concept that is currently being investigated: the Wide Area Augmentation System (WAAS), the Local Area Augmentation System (LAAS), and the conceptual free-flight system. These systems and the free flight concept are envisioned to eventually replace the current national system that relies on air traffic control radar systems, ground based VOR Stations, and on-board aircraft magnetic compass and inertial navigation systems. Figure 1 is a simplified artist's rendition of the WAAS system.

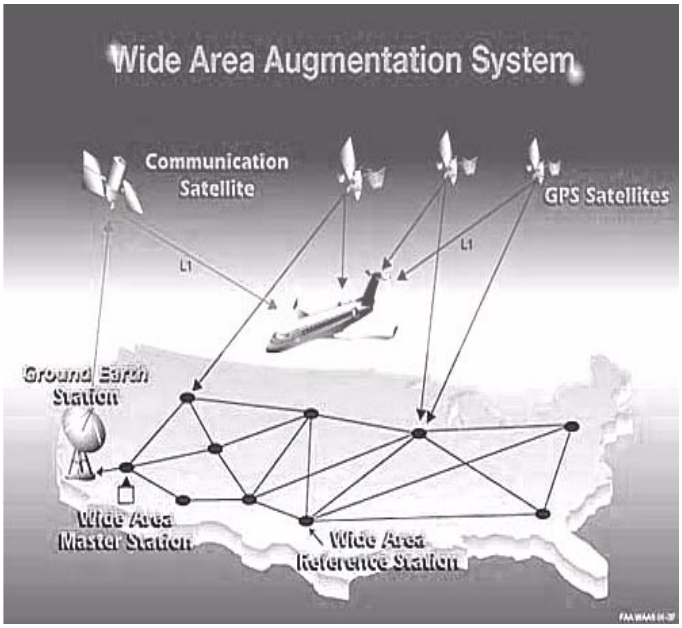

Figure 1: Sketch of Wide Area Augmentation System (WAAS) - general concept.

The free-flight operational concept is the most speculative at this time and is undergoing intensive study. The overall concept of free flight is to empower aircraft pilots to choose their flight paths and not be totally controlled by ground-based

traffic controllers. The GPS makes it technically feasible for every aircraft to know where it is in relation to other aircraft that may pose a threat.

The WAAS is an evolving system but has some general characteristics (Ref. 2) The WAAS relies on GPS to provide positional information to receiving aircraft flying over the continental U.S., and as such could be used for free-flight navigation. A fully implemented WAAS though could also be use to implement Category 1 landings. In some cases, these are automatic computer controlled runway approaches until the aircraft reaches an altitude of 200 feet above the runway and a forward visual sighting of 1500 feet. At this point, the pilot manually lands the aircraft. The LAAS is a similar system but requires greater landing accuracy than WAAS to enable Category 2 or 3 landings for a local area within 20 miles of a LAAS equipped airport. A Category 3 landing includes a zero distance runway visibility which requires automatic control through aircraft roll-out.

During the preliminary design of the WAAS system, a number of candidate architectural system designs were investigated. Because a malfunction in the WAAS system could lead to a loss of life, the reliability of the system was investigated. This paper describes the analysis of one such system which used a unique sparing scheme to enhance reliability and reduce spacecraft costs. The importance of this exposition, however, lies not in the system architectural design itself but rather in the technique that was used to predict the system reliability. A better understanding of this WAAS system design is necessary though before the solution technique can be best appreciated.

GPS receivers used for recreational civilian applications require access to a minimum of four GPS satellites which are typically available. However, in order to meet acceptable signal integrity for all phases of flight (without WAAS), the aircraft receiver must perform Receiver Autonomous Integrity Monitoring (RAIM) which requires a minimum of five GPS's. The accuracy of positional data is 100 meters (95% confidence) and presents too large an uncertainty for precision approach and landings. A technique called differential GPS can reduce the error down to centimeters by using range corrections from a differential GPS station. The WAAS as currently envisioned will utilize 35 known reference stations distributed throughout the continental U.S. These reference stations also receive GPS positional data, and because each station knows its coordinates exactly, it can compute timing errors contributed by the atmosphere, the receiver's internal clock, and satellite clock and ephemeris (where the GPS thinks it is) errors. These errors are then broadcasted as corrections to WAAS users so they can be applied to the measurements on the aircraft. The result is a position solution with improved accuracy. The WAAS corrections are expected to result in a solution accurate enough to meet the requirements for Category 1 approach and landing.

For Category 2 or 3 operations. LAAS will be required in order to meet the requirements for accuracy, availability, continuity, and integrity. LAAS consists of a local reference station broadcasting corrections that allows aircraft to generate position solutions accurate enough for all categories of approach and landing.

The WAAS system as currently envisioned is comprised of aircraft with GPS/WAAS receivers and transmitters, the ground-based reference stations, the GPS satellites, and three additional WAAS geosynchronous satellites (GEO's). Since the reference stations are distributed throughout the U.S., an up-link transmitter and a broadcasting satellite are needed. The system works as follows: Aircraft and reference stations receive GPS positional data, the reference stations transmit their correction data to a ground-based satellite up-link station, that transmits the correction data to a geosynchronous WAAS communications satellite that in turn broadcasts the data to all aircraft flying over the continental U.S. These aircraft are able to generate position solutions that enable them to perform precision approach and landing operations (at or near Category 1 minimums) throughout most of the continental U.S. Because of reliability and safety concerns, redundant systems are employed.

CANDIDATE WAAS ARCHITECTURE

Early in the conceptual design phase of the WAAS, a number of candidate architectures were studied. This paper addresses one of them that presented a particularly interesting reliability modeling challenge from the model solution viewpoint. The candidate WAAS geosynchronous satellite communication system studied and reported in this paper differs from the current FAA WAAS system primarily in the way the WAAS satellites are positioned in their equatorial orbits, their number, and their respective signal coverages. Also, the satellite failure distributions for this study are representative data and may not accurately emulate the Immarsat (Ref. 3) satellites planned for the initial WAAS implementation.

The particular WAAS-like system that was studied requires two GEO's to adequately cover the near-U.S. airspace; however, only one operational satellite is required for the system to be operational to just cover the continental U.S. Since this satellite system is critical for precision approach and landings requiring a very high reliability, three redundant satellites serve as hot spares bringing the total number of GEO's to four. Figure 2 shows one possible signal coverage for the four WAAS-like satellites. With this coverage pattern, three redundant satellites provide additional coverage for Pacific and Atlantic coastal traffic. The GEO's have the capability to be repositioned in orbit which adds further flexibility in defining the covered pattern; however, the GEO's provide other communications services that limit that flexibility and therefore their repositioning capability was ignored in this study. The unique feature of this system model comes into play when the system degrades due to three GEO failures. The construction of a fifth GEO, the build-GEO, would immediately begin and is launched upon completion. The time to build the replacement

GEO for this assessment was considered to be stochastic with a Weibull distribution.

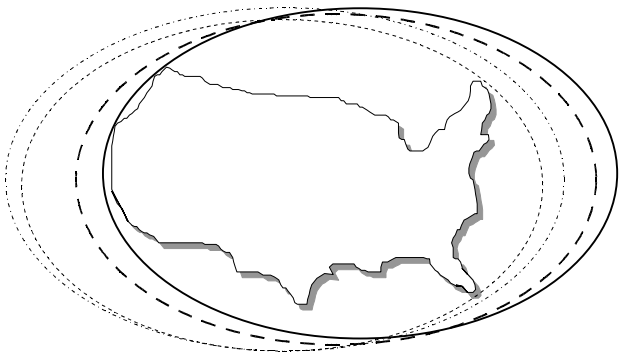

Figure 2: WAAS-like GEO signal coverage for continental U.S

The mean build-time is 4000 hours, approximately six months, with a standard deviation of 2050 hours, about three months. The reliability assessment task was to determine the probability that the fourth operating GEO would fail before the fifth GEO was constructed and launched. The model for this system is called the build-model.

Because the build-GEO acts like a cold spare with a non-constant failure rate, the reliability model for this system is non-Markovian and cannot be solved with standard Markovian techniques. Such reliability models are non-Markovian because the model requires multiple clocks. One clock keeps track of component failures which starts at the initiation of the mission, the second clock starts at the initiation of the build-GEO construction, and the third starts when the cold Weibull spare is fully powered, i.e., when switched on. The general mathematical model which describes these systems is given by the Chapman-Kolmogorov equations (Ref. 4). Presently, the most practical solution methodology for such models is Monte Carlo simulation. A combination of two new technologies now makes it feasible to arrive at reliability predictions for these non-Markovian models. The first is a modeling technology that allows one to describe this non-Markovian model with a simple dynamic fault tree notation first developed for the Hybrid Automated Reliability Predictor (HARP) (Ref. 5). The fault tree is dynamic because it is not restricted to combinatorial events. The dynamic switching behavior of the spare build-time and the switching-in of the cold Weibull spare is made possible by using the unique sequence enforcing fault tree gate. The second technology to be used is the importance sampling method in the Monte Carlo simulation (Ref. 6). Importance sampling is a variance reduction technique that makes the sampling of system failures very efficient; drastically reducing the execution time by orders of magnitude in most cases and in particular for very high reliable systems.

MONTE CARLO INTEGRATED HARP

By the end of 1990, a prototype Monte Carlo HARP computer program was developed by researchers at Northwestern University under grant to NASA Langley (Ref. 7) . The idea of structuring the simulation based on the Markov chain was first presented to me by Robert Geist at Clemson University Ref. 8). Northwestern researchers implemented a similar concept using the HARP program's fault/error-handling models. Mark Boyd (a HARP codeveloper now at NASA's Ames Research Center) further integrated the Monte Carlo simulator with HARP's fault tree notation, and I later reengineered the program to be consistent with HARP (now called Monte Carlo integrated HARP, i.e., MCI-HARP). With a working program on hand, Boyd and I tested MCI-HARP's ability to explore the effects of decreasing failure rates with warm and cold spares on a Jet Propulsion Laboratory's proposed guidance, control, and navigation system, a 3-dimensional hypercube fault-tolerant system applicable to a manned mission to Mars (Refs. 9, 10, 11).

WAAS-LIKE FAULT TREE MODELS

The GEO's contain redundant components and exhibit an increasing Weibull hazard rate given by:

$$H(t) = \lambda\alpha t^{\alpha-1} \qquad \text{where } \alpha = 1.5 \text{ and } \lambda = 3.8X\ 10^{-9}$$

In order to get a rough estimate of the system reliability using straight forward solution techniques that could be confirmed with an analytic solver, two simplified models were initially used. The all-hot model consisted of five operational GEO's; all with Weibull hazard rates using the λ and α values previously defined. This model should produce a pessimistic upper bound on the system reliability relative to the build-model. The fault tree model for the all-hot system is simply an AND gate with five basic events representing GEO failures.

The second model, bad-as-old model, also contains five hot GEO's but unlike the all-hot model, a fifth GEO is precluded from failing until three hot GEO's have failed. The bad-as-old model is analogous to installing a used but functional part in a machine. To model this system, a dynamic fault tree model is required.

The dynamic fault tree model for the bad-as-old system is shown in figure 3 andpears straight forward except for the sequence enforcing gate.

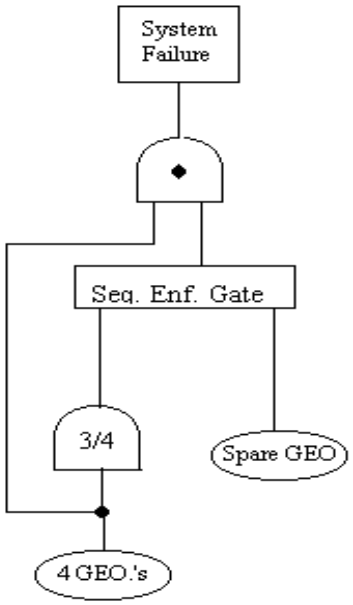

Figure 3: Bad-as-old and good-as new fault tree model

This unconventional gate makes the fault tree dynamic in that it forces its input events to occur in a specific order. The AND gate, by contrast, places no conditions on the order of its input events to fire the gate. Only the combinatorial binary input values matter. The remaining gate is a 3 out of 4 gate which fires when any three of the four input events have occurred. The single input line is shorthand notation for four independent input events which represent the four operational GEO's. When any of the three operational GEO's have failed, the ¾ gate fires and enables the sequence enforcing gate. The spare GEO is switched in and becomes operational. After this time, either the fourth operational GEO fails or the operational spare can fail. Only after they both fail, will the AND gate fire declaring a system failure.

When this model is solved using an analytic solver (HARP's Markov chain solver in this case), only one mission time clock inherent in the Markov chain model is allowed. Consequently, the hot spare's clock is automatically set to the mission time clock. The subtle effect is that the hot spare instantaneously remembers its past history, and it ages, even though it was precluded from failing up until the switch-in time. Intuitively, one would expect the unreliability of this system to be somewhat less than the all-hot spare model.

The third model precludes the spare from remembering it's past and is therefore a cold spare. This good-as-new model is analogous to replacing a faulty machine component with a brand new one. As applicable to a WAAS-like system, the cold spare GEO could be launched with the others but kept unpowered. Another possibility could be that the cold spare GEO would be waiting on a launch vehicle and launched when three GEO's in orbit fail. The fault tree for the good-as-new model is identical to the previous bad-as-old fault tree (figure 3) except that this model is no longer Markovian and cannot be readily solved analytically because two clocks are now required. One tracks the system mission time as before, while the second starts at its zero time when the cold spare is powered up. A non-Markovian model requires a much more complex analytical solution than the previous models. Monte Carlo simulation is ideally suited to solving non-Markovian models and was chosen in lieu of an analytical solution. The addition of the second clock occurs naturally in the Monte Carlo simulation when the sequence enforcing gate is included. The unreliability was estimated using MCI-HARP and one would expect the result to be better than the previous two, a lower unreliability.

The last model studied is a variation of the good-as-new model, but allows a stochastic delay representing the time required to build and launch the cold spare GEO. The fault tree is similar to the good-as-new model with four additional gates and one additional input to the sequence enforcing gate to account for the build-delay. Figure 4 depicts the model.

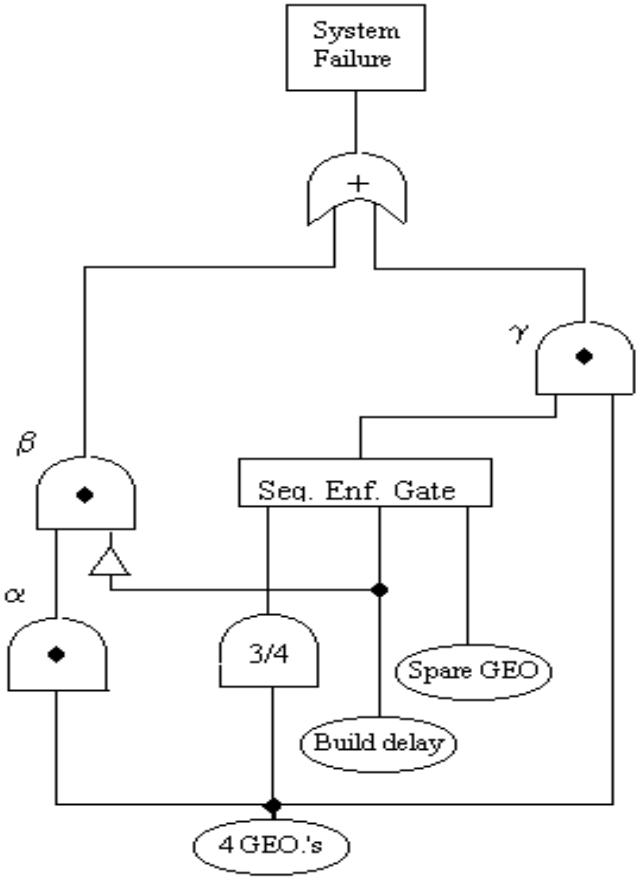

Figure 4: WAAS-Like fault tree model

The build-delay event is represented by a Weibull distribution with $\lambda = 4.95X10^{-8}$ and $\alpha = 2.0$. This distribution has a mean of 4000 hours (about six months) and a standard deviation of 2050 hours or about three months. This fault tree model requires three clocks with two serving the same function as for the good-as-new model while the third clock tracks the build-time. Like the good-as-new model, the build-model is

non-Markovian and required the MCI-HARP for solution. The unreliability for this model accounts for the race condition that commences when the third GEO fails leaving one operational GEO in orbit and one that immediately begins construction for deployment before the last orbiting GEO fails.

An explanation of the operation of the fault tree in figure 4 follows: After three operational GEO's fail, the sequence enforcing gate enables the build-time event which is a stochastic clock that immediately starts. Two possible events can now occur: The fourth operational GEO can fail or the build-time clock event occurs. If the fourth GEO fails, the α AND gate fires and enables one of two inputs to the β AND gate. Since the build-time event hasn't occurred, the invert gate fires causing the β AND gate to fire and in turn the top OR gate to fire signifying system failure. The system failed because all four orbiting GEO's failed before the cold spare GEO was launched. If the build-time event occurs before the fourth operational GEO fails, then the β AND gate is disabled precluding a system failure if the fourth GEO now fails. The spare GEO event is immediately enabled which means construction was completed and the spare GEO is launched and became operational. At this time, either the fourth GEO fails or the operational spare fails. If the spare fails first, the sequence enforcing gate fires enabling one γ AND gate input. When the fourth GEO fails, the γ AND gate fires signaling system failure through the OR gate. If the fourth GEO fails first, one input to the γ AND gate is enabled. When the spare fails the sequence enforcing gate fires causing the γ AND gate to fire signaling system failure through the OR gate. Intuitively, one would expect the unreliability to be greater than the good-as-new model but better than the all-hot model.

The unreliability results for all models were evaluated at 80,000 hours. For the all-hot and bad-as-old models, solutions were obtained using the analytical engine in HARP and the Monte Carlo simulation engine in MCI-HARP where both solution engines are valid uses for these models (Only one system clock is required.). The execution times are given for a Pentium 200 Mhz PC running in the Windows 95 environment.

Unreliability Estimation Summary

	All-hot	Bad-as-old	Good-as-new $^{\Delta}$	WAAS-like $^{\Delta}$
Unreliability	* 3.8×10^{-6} $^{\Delta}$ 3.8×10^{-6}	* 1.6×10^{-6} Ξ	0.75×10^{-6}	1.3×10^{-6}
Std. dev.	+/- $^{\Delta}$ 0.08×10^{-6}	Ξ	+/- 0.02×10^{-6}	+/- 0.2×10^{-6}
No. trials	$^{\Delta}$ 0.5×10^{5}	Ξ	10^{5}	10^{5}
Run time	< *1sec $^{\Delta}$ 19sec.	< *1sec Ξ	50 sec.	60 sec.

* HARP analytic solution (model setup time excluded)

Δ MCI–HARP simulation (model setup time excluded)

Ξ MCI-HARP use produces Good-as-new data

DISCUSSION OF RESULTS

As expected, the all-hot model produced the highest unreliability (an upper bound), but surprisingly, not significantly greater than the bad-as-old model that precluded failure of the last hot spare. The good-as-new model which assumes instantaneous operation of a cold spare with no build-time produced the lowest unreliability (a lower bound). The WAAS-like model shows an unreliability greater than the good-as-new model but less than the others. This result is expected as it accounts for the possibility of the last operational GEO failing before the build-GEO is constructed and launched. The data suggest that the delay in building and subsequently launching the cold spare is a reasonable strategy based on the slight increase in unreliability over an immediate launching of an available cold spare. Results data are given for the HARP analytic engine and the MCI-HARP simulation engine for the all-hot and bad-as-old models. As expected, comparable

results are given. For these simple models though, the analytical engine is lightning fast.

CONCLUDING REMARKS

A remarkable feature of the MCI-HARP is that the simulation code did not need to be changed to solve the non-Markovian models. The robustness of the dynamic fault tree notation and flexibility of the Monte Carlo simulation made it easy to obtain solutions. The concept of evaluating the build-time and hence the launching of a cold spare GEO's effect on system reliability produces a novel fault tree model and was shown to be straight forward to assess.

One other observation is worth noting here and regards the use of the Weibull distribution and the ability of MCI-HARP to model and solve systems which are characterized by them. The modeling of these systems commenced with the Weibull failure distributions of the GEO's and took full advantage of the results of some other reliability program's computed results. The GEO's are very complicated fault-tolerant systems that use substantial redundancy to achieve ultra-high reliability, but because MCI-HARP has the ability to model the GEO's with the Weibull distribution, it was unnecessary to include the massive detail of the GEO's architecture. The Weibull model captured all the necessary detail in a simple distribution making the WAAS satellite system easily modeled and solved.

The price paid for that capability is over an order of magnitude increase in computation time for the precision (standard deviation) required over the analytical solution. The higher the precision, the longer the run time. For semi-Markov models requiring multiple time clocks, Monte Carlo simulation with importance sampling is often the only practical choice. The choice of solution engines for Markovian models with non-constant failure rates requiring only one clock is less straight forward as there isn't a linear relationship between the size of the model and computation time. When component failure rate distributions produce state transition rates that differ markedly, analytic solution engines become less attractive and Monte Carlo more so. For now, both solution techniques are valuable; however, computers are running faster and getting cheaper each year. Monte Carlo simulation with all it's potential computational power appears to have a bright future for reliability prediction.

REFERENCES

1. http://www.faa.gov/and/and500/and510/gps-aug/augs.htm
2. http://www.trimble.com/gps/fsections/aa_f1.htm
3. http://www.inmarsat.org/inmarsat/
4. Cox, D.R. & Miller, H.D., The Theory of Stochastic Processes, John Wiley & Sons, 1965
5. Bavuso, S.J., et. al., HiRel: Hybrid Automated Reliability Predictor Tool System (Version 7.0), 4 vol.s, NASA TP 3452, Nov. 1994
6. Lewis, E.E., & Bohm, F., Monte Carlo Simulation of Markov Unreliability Models, Nuclear Engineering and Design 77 (1984) 49-62 North-Holland, Amsterdam
7. Platt,M.E., Lewis, E.E., & Boehm, F., General Monte Carlo Reliability Simulation Code Including Common Mode Failures and HARP Fault/Error Handling, NASA Contract Report 187587, Jan. 1991
8. Geist, R.M. & Smotherman, M.K., Ultra Reliability Estimates Through Simulation, Proc. Reliability & Maintainability Symp., 1989 (350-355)
9. Boyd, M.A. & Bavuso, S.J., Simulation Modeling for Long Duration Spacecraft Control Systems, Proc. Reliability & Maintainability Symp., 1993 (106-113)
10. Bavuso, S.J., Aerospace Applications of Weibull and Monte Carlo Simulation with Importance Sampling, Proc. Reliability & Maintainability Symp., 1997 (208-210)
11. Bavuso, S.J., Aerospace Applications of Weibull and Monte Carlo Simulation with Importance Sampling, Proc. Reliability & Maintainability Symp., Computer-Aided Engineering Workshop, Vol.2, Panel 10D, 9 pp.s, 1997

BIOGRAPHY

Salvatore J. Bavuso

WORK: NASA Langley Research Center
MS 130
Hampton, VA 23681-0001, USA
(757) 864-6189
FAX: (757) 864-4234

Salvatore (Sal) J. Bavuso is a senior researcher at NASA Langley Research Center in Hampton, Virginia. He received the BS degree in mathematics from the Florida State University in 1964 and the MS degree in applied mathematics from the North Carolina State University at Raleigh in 1971. He has been instrumental in the development of advanced reliability modeling technology for over two decades. He was the NASA project manager for and a codeveloper of the HiRel, HARP, and CARE III programs. For more information see:
http://tnasa.larc.nasa.gov/~atbse/se_group.html